THE DEFENSIVE INFORMATION OPERATIONS OFFICER AT THE JOINT TASK FORCE

By
Major Frederick C. Hellwig, Armor, USA
And
Captain Boyd R. Plessl, Signal Corps, USA

JTF 2002 SITREP Extracts:

" 0210 Zulu, 2 June 2002 Unclassified JFACC Web sites in Theater are defaced by anti-US propaganda. International news media report success of Hacker group against US Forces. Hacker groups threaten further attacks unless JTF Forces withdraw from the Area of Operations. "

" 1835 Zulu, 5 June 2002 JTF Logistical staff planners lose classified data on all ammunition requirements for the Theater because of computer equipment failure. Due to insufficient data back-up procedures JTF planners require 65 hours to recover from the damage. JFLCC ammunition shortages continue."

" 2345 Zulu, 6 June 2002 adversary controlled radio and television stations in the JTF Area of Operations report false propaganda claims that JTF forces are conducting computer network attacks against public services (water, power, telephones, and hospitals) resulting in 137 civilian deaths. Within 50 minutes Reuters, AP, CNN, and the BBC are running related stories with adversary provided video from the effected areas."

" 0340 Zulu, 7 June 2002 DISA's Joint Web Risk Assessment Cell informs the JTF that portions of two JTF OPLAN annexes were found on unclassified sites. Additional Sensitive But Unclassified (SBU) items that violate OPSEC guidance were also found."

" 1554 Zulu, 7 June 2002 the Fleet unclassified e-mail server is hit by a distributed denial of service attack. Server is off line for 15 hours. Original source of the attack is under investigation."

" 1615 Zulu, 7 June 2002 network intrusion detection systems (IDS) at the Regional CERT alert on attempted mapping of JTF networks. The CINC directs the JTF to go to INFOCON BRAVO (Specific Threat) and report on all actions implemented to secure information and information systems."

" 1327 Zulu, 8 June 2002 a computer virus is detected on the JTF's unclassified network. Several systems have reported files deleted from their hard drives."

Figure 1

Defensive Information Operations Doctrine

Tactical Commanders have always placed a premium on detailed, timely, and accurate information upon which to base their decision making processes. Joint doctrine (JP 3-13) clearly states that Information Operations (IO) are critical to achieving and sustaining the information superiority required for decisive Joint Operations. Our increasing reliance on information systems and networks to deliver vast quantities of relevant information to the Joint Task Force (JTF) commander and his staff in real time has also exposed new vulnerabilities that demand attention.

JTF Commanders face an increasingly capable, sophisticated, and varied array of asymmetrical threats to our hold on information superiority. The potential for intrusions, malicious viruses, and attacks against our information systems and networks exists throughout the continuum of peacekeeping through war, and return to peace. Integrated JTF level defensive IO planning from the initial planning stages through mission completion and redeployment of forces is an essential component of all JTF missions. The Joint Pub 3-13, Joint Doctrine for Information Operations, definition of defensive information operations states:

> **Defensive Information Operations.** The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Defensive information operations are conducted through information assurance, physical security, operations security, counter-deception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations. Defensive information operations ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (Joint Pub 3-13)

Figure 2

The Defensive Information Operations Officer

The first step in addressing the need for defensive IO planning is to identify early in the JTF activation process a Defensive Information Operations Officer (DIO) assigned within the J9 (IO Staff). IO planning and specifically defensive IO must be integrated

from the on set of the JTF planning effort. If a Joint Planning Group (JPG) is formed prior to the activation of the full JTF, the DIO must be part of the initial JPG staff. The actual DIO may be member of the headquarters designated as the JTF or may be a qualified individual requested from the Joint Information Operations Center (JIOC) or Service Information Warfare Center (LIWA, FIWC, AFIWC). The JTF DIO's duty description should state;

"Responsible for the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. Coordinate the activities of Information Assurance (IA), INFOSEC, Computer Network Defense (CND), Physical Security, OPSEC, counter deception, counter propaganda, CA, and PA. Assist the J6 staff in the preparation and review of the Information Assurance Appendix to the Communications Annex. Assist the J3 in the preparation of the OPSEC Appendix, and assist the J2 in identifying threat IO capabilities. Participate, as a full time member, of the J9 Information Operations Working Group (IOWG). Provide input to the Information Operations Appendix to the Operations Annex. Serve in the position of Deputy J9 as required."

The DIO duty description proposed above requires an extensive breath and depth of experience in Joint staff operations, JOPES, and several IO related specialty areas that will necessitate a field grade officer (O4 or higher). The DIO must also bring an in depth knowledge of the threats to the JTF's information and information systems and a solid understanding of the available countermeasures that may be employed in defense of the JTF's networks. In designating a JTF DIO, the JTF Commander must choose an individual who is also intimately familiar with our own friendly systems and network common vulnerabilities. The JTF DIO may consider requesting a full scope holistic IO Vulnerability Assessment of the JTF to fully evaluate the defensive IO posture of the Command. (See Cyber Sword, Spring 2000, Winning the Information War Before It's Fought.)

OPSEC and the Defensive IO Officer

OPSEC is a potential Achilles heel for any large complex organization. This is particularly true for a Joint Task Force that must rapidly incorporate several service components and begin the planning process under time pressure. Often, the JTF Defensive IO Officer will be the designated as the OPSEC officer. He should be school trained and knowledgeable in OPSEC doctrine and tactics, techniques, and procedures (TTP). The Defensive IO Officer should immediately implement an aggressive OPSEC Awareness and training program throughout the JTF. The Interagency OPSEC Support Staff (www.ioss.gov) is an excellent source of readily available materials that can be used to get an OPSEC Training Program off the ground rapidly. They will provide training films, posters, regulatory guidance, on site training, OPSEC surveys and program checklists.

In addition to the mandatory Public Affairs Officer (PAO) review of press releases and development of media ground rules, all forms of information released into the public domain should be subjected to a thorough OPSEC review. Strict command policies memorandums must be established to control the proliferation of web sites and the information and digital images that appear on these sites. The DIO should review the Center for Army Lessons Learned (CALL) IO TTP (http://call.army.smil.mil), the LIWA homepage lessons learned (http://www.liwa.army.smil.mil), and the Joint Information Operations Center IOJULL's (http://iojulls.jc2wc.aia.kelly.af.smil.mil). Internet access should be tightly limited to only those sites that are required. As the OPSEC proponent on the JTF staff, the DIO in conjunction with the J3 will develop the JTF's statement of essential secrecy, critical information list, and Essential Elements of Friendly Information (EEFI) that must be protected. The DIO and J3 should include mission specific EEFI in all orders issued by the JTF.

The DIO should request JICMA monitoring of all telephonic, wire, cellular and voice mail communications early in the JTF stand-up process. The monitoring summaries provide excellent feedback on the effectiveness of the training program and they can be used at the evening shift updates to maintain OPSEC awareness among the staff.

Countermeasure Recommendation/Implementation

Every JTF is unique and will have it's own particular IO vulnerabilities and concerns. The DIO must work closely with other JTF staff elements to eliminate or mitigate these vulnerabilities. Close coordination with the J2, J3, and J6 in vulnerability reduction is essential for the DIO to be effective. Command support is critical to affecting a more secure IO posture. Several years of DOD experience in contingency operations implementing defensive IO has produced a number of cost and time effective measures. Some of the common countermeasures that DIO's should consider recommending and implementing when assessing their defensive IO posture are listed below.

- Establish and vigorously enforce network SOP's and policies (User, System Administrator, and ISSM).
- Review all network architecture changes for security impacts. Effective CND relies on several overlapping layers of defense (Firewalls, Routers, Intrusion Detection Systems, solid user password selection/protection, and limits on user network privileges).
- Increase INFOCON levels in response to the operational environment. Changes in the JTF's INFOCON level will be closely tied to the threats that the JTF anticipates facing. Develop specific network defensive measures for each level of INFOCON and prepare both internal and external reporting procedures.
- Obtain and utilize security software to ensure internal network security against potential trusted internal user threats. Utilize auditing, network protocol analysis, and system monitoring practices. Reviews these logs daily.

- Ensure compliance with all DISA and Service CERT Information Assurance Vulnerability Alerts (IAVA's). (Application of all the latest operating system fixes and patches)
- Establish and maintain daily contact with the Regional CERT. The Regional CERT will be a critical resource for the DIO's and J6's information assurance efforts.
- Implement a comprehensive anti-virus program. Check A/V updates on all hosts at least weekly and more frequently when viruses are detected. Updates to the anti-virus files are available through the RCERT, ACERT, and DISA. Disseminate computer virus reporting procedures to the JTF. Train AIS users to isolate and scan email attachments.
- Conduct regular system back-up of network information to facilitate quicker recovery from system failure due to malicious attack or natural disaster. Store back-up information in a physically separate location in a fire and flood proof container.
- Request/conduct periodic IO Vulnerability Assessments of the JTF. Utilize automated network vulnerability scanning tools.
- Train and certify AIS users prior to the issuance of an account on any network. Reinforce this training regularly. AIS user certification is just as critical and potentially more dangerous to the JTF than the failure to properly license vehicle operators.
- Ensure a security baseline is established and enforced for all AIS in the JTF headquarters including which Operating Systems (OS) will be supported by the J6 (Windows 95, 98, NT, 2000 and others). All systems must be inprocessed through the J6 for security "hardening". The "default" or "out of box" configuration is inherently unsecure.
- Continuously monitor security on the JTF's web sites. Limit the write ability so only a limited number of personnel can write to the web sites.
- Coordinate with the J6 for a ".com" Internet connection to assist the PSYOP, CA and PAO officers with target audience research and other information requirements. This will help protect this Internet search activity from being traced to a .mil address, thus providing an indicator of the JTF's mission.
- Conduct reaction drills and rehearsals with the PAO, PSYOP, and Civil Affairs staffs to decrease JTF response time to adversary propaganda operations and adverse media events. Draft on the shelf press releases, foreign language products and local media radio/TV spots for counter propaganda operations.
- Enforce strict use of password protected screen savers, and warning banners throughout the JTF.
- Review all Freedom of Information (FOIA) requests submitted to the JTF and the responses for OPSEC.
- Request and disseminate updated SATRAN and Open Skies over flight information.
- Request the Joint Web Risk Assessment Cell and Service Information Warfare Center capabilities to review Open Source Intelligence review of JTF EEFI in the public domain.
- Ensure all AIS are power surge protected.
- Set all STU III's in the JTF planning cells and classified areas to the auto secure function. Enforce use of secure communications.

- Restrict access to commercial capable phones to minimize inadvertent compromise of EEFI. Post the EEFI clearly around all telephones in the JTF Headquarters
- Segregate classified from unclassified machines. Mark all media throughout the headquarters clearly (printers, CPU's, monitors, copiers, FAX machines, telephones). Limit Internet access to specific machines in each staff section or element and physically segregate (air gap) these machines from the rest of the networks.
- Maintain strict physical security. Do not allow free access throughout the Headquarters to civilian cleaning teams. Establish specific morning and afternoon clearing hours and then escort local national cleaning personnel.
- Do not locate telephone switches, computer hubs, and other communications equipment in unsecured areas that can be accessed by non-US personnel. (Cleaning closets, maintenance rooms, ECT.)
- Remove all old and excess cabling. Active cable should be tagged (color coded not by name) and placed on telephone poles. Conduct periodic wire walks by the guard force (minimum twice per day) to ensure no taps or barrel connectors have been placed on the network lines. Replace old cable with fiber-optic cable.
- All removable electronic media should have proper classification markings. Check all outgoing media for proper security wrapping and courier orders. Provide the guard force a stand-alone computer (not connected to the network), A/V software, and a "Dirty Word" search tool at the exit/entry point to checks all storage media. Ensure guard force personnel check electronic media (laptops, floppy disc, zip disc, digital cameras, ECT) coming into the Headquarters.
- Conduct weekly perimeter checks of the Headquarters compound for suspicious unmarked cables.
- Develop, use and enforce a Security Classification Guide throughout the Joint Task Force.
- Challenge all unknown personnel badged or unbadged that are working in proximity to JTF AIS equipment.
- Burn or shred all office waste paper completely. Conduct frequent dumpster diving operations. Don't place trashcans near or around copying machines. Properly account for and destroy all unnecessary copies of orders, annexes, and drafts.

The Defensive Information Operations Solution

The solution to the Defensive Information Operation challenge does not lie in any one specific security discipline. The successful Defensive Information Officer will utilize a mixture of traditional intelligence gathering, OSINT, OPSEC, COMSEC monitoring, Physical Security, Command Policy Memorandums, SOP's, COMPUSEC, Information Assurance, Electronic Warfare, PAO, Civil Affairs, PSYOP, and counter propaganda tools to improve the defensive posture of the JTF. The JTF's information environment will always be in a state of constant change. Personnel, equipment, software, and changing threat capabilities require the DIO to constantly revisit all security areas and concerns.

A detailed IO Risk Assessment and Risk Management are required to commit the DIO's limited security resources to the task of protecting the JTF's Information and Information Systems. JTF Command Group support for the DIO's initiatives and disciplined execution by commanders at all levels of the JTF are critical to achieving and maintaining information superiority. The ability to work successfully with the other JTF staff sections to implement innovative solutions is a prerequisite for effective Defensive Information Operations.

Major Hellwig is currently assigned as the Land Information Warfare Activity's Chief of Current Operations. A career armored cavalry officer, he has served previously as an Information Operations Vulnerability Assessment Team Chief conducting assessments in Germany, Bosnia, Korea, Italy and numerous CONUS installations, and as a JTF IO Defensive Information Officer. A graduate of CGSC, the Army OPSEC Course, the Joint PSYOP Planners Course, the USAF IW Course, and the Joint Information Warfare Staff Operations Course, he has served in command and staff assignments in the 2nd Armored Cavalry Regiment, 3-7th Cavalry, 78th Division, 8th Infantry Division (Mechanized), and the 82nd Airborne Division.

CPT Plessl is currently assigned as the Operations Officer for the Information Operations Vulnerability Assessment Division of the LIWA. A Signal Officer, he has served as a Deputy IO Vulnerability Assessment Team Chief for numerous CONUS and OCONUS assessments of tactical Army Commands. He has also participated as a member of Joint assessments in support of the Joint Information Operations Center. He has served in command and staff positions in the 3rd Infantry Division, 40th Signal Brigade, and the Army Signal Command.